**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

I, Craig S. Mehrmann, a Special Agent of the Federal Bureau of Investigation, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application for a warrant to search for information associated with the following account:

   a. User identification ("UID") number 459434556081176576, username "bokunobubbles#0" ("TARGET ACCOUNT ONE"), account email address kuhaspolchies@yahoo.com, which is believed to have been utilized by Kuhas Polchies ("Polchies"),

which is stored at premises controlled by Discord, Inc. ("DISCORD"), an electronic communications and remote computer services provider which accepts service of legal process at 444 De Haro St., Suite 200, San Francisco, CA, 94107.

2. I describe the information to be searched in the following paragraphs and in Attachment A. I make this Affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require DISCORD to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since February 2023. I am currently assigned to the Boston Division, Portland, Maine Resident Agency, of the FBI. As part of my duties, I investigate crimes involving the sexual exploitation of minors, including the production, possession, and distribution of child

pornography. I have received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children. As a Special Agent, through my training, education, and experience, I have become familiar with the efforts of persons involved in criminal activity to avoid detection by law enforcement, to include matters involving sexual exploitation of children. I have worked and consulted with highly experienced law enforcement professionals who are skilled in working cases involving sexual exploitation of children. I have received training on the proper investigative techniques for these violations, including the use of surveillance techniques and the application and execution of arrest and search warrants.

4. The information contained in this affidavit is based on my personal knowledge, as well as information relayed to me by other law enforcement agents and officers involved in this investigation.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, U.S.C § 2251(a) (sexual exploitation of children), 2252A(a)(5)(B) and (b)(2) (possession of and access with the intent to view child pornography), AND 2252A(a)(2) and (b)(1) (receipt or distribution of child pornography), have been committed by Kuhas Polchies. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

## JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States…that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

## STATUTORY AUTHORITY

8. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252 and 2252A, relating to material involving the sexual exploitation of minors. Based upon my training and experience, I know the following:

a. 18 U.S.C. § 2251(a) in pertinent part prohibits a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in, or having a minor assist any other person to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, if that visual depiction was produced or transmitted using materials that have been mailed, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. It is also a crime to attempt to violate 18 U.S.C. § 2251(a).

b. 18 U.S.C. § 2252(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails.

c. Under 18 U.S.C. § 2252(a)(4), it is a crime for a person to knowingly possess or knowingly access with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, or have been shipped or transported using any means or facility of interstate or foreign commerce or in and affecting interstate or foreign commerce, or which were produced using materials which have been mailed or so shipped or transported, by any means including by computer.

d. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(3) prohibits a person from knowingly reproducing child pornography for distribution through the mails or in or affecting

interstate or foreign commerce by any means, including by computer. Under 18 U.S.C § 2252A(a)(3)(B), it is a crime for a person to knowingly advertise, promote, present, distribute, or solicit through the mails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains an obscene visual depiction of a minor engaging in sexually explicit conduct, or a visual depiction of an actual minor engaging in sexually explicit conduct. Under 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

**DEFINITIONS**

9. The following definitions apply to this Affidavit:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, illegal or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used herein, includes the definitions in 18 U.S.C. §§ 2256(8) and 2256(9) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). See 18 U.S.C. §§ 2252 and 2256(2).

c. "Visual depictions" include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in permanent format. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic or storage functions,

and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form, or electrical, electronic or magnetic form, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Digitally 5coded data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also

encrypt, compress, hide, or "boobytrap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet and is associated with a physical address. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) may assign a unique and different number to a computer at different times that it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

j. "Wireless telephone" (or mobile telephone, or cellular telephone, or smart phone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining

the location of the device. Many wireless telephones are minicomputers or "smart phones" with immense storage capacity.

k. A "digital camera" is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

**COMPUTERS AND CHILD PORNOGRAPHY**

10. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and computer forensic examiners, I know that computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. In the past, child pornography was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and significant skill to develop and reproduce the images. There were definable costs involved with the production of pornographic images, and to distribute these images on any scale required significant resources and significant risks. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public and/or law enforcement. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

11. The development of computers has radically changed the way that child pornographers manufacture, obtain, distribute, and store their contraband. Computers basically serve five functions in connection with child pornography: access, production, communication, distribution, and storage.

12. Digital cameras, as well as "smart" phones, have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras have the capacity to hold hundreds of images and videos. A modem allows any computer to connect to another computer using a telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers worldwide.

13. As is the case with most digital technology, communication by way of computer can sometimes be recovered from a forensic examination of the computer used for these purposes or by obtaining stored information from the electronic communication service provider. Often electronic communication service providers save transcripts or logs of electronic communications between users that have occurred over the Internet. These logs are commonly referred to as "chat logs." Some programs allow computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as "chatting," or "instant messaging." Based upon my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they can record communication in transcript form, often show the date and time of such communication, and may also show the dates and times when images of child pornography were traded over the Internet.

## INFORMATION REGARDING DISCORD

14. In my training and experience, I learned that Discord was launched in May 2015 and specifically marketed towards the "gaming" community. The service features a desktop application as well as a mobile application, and a user will typically use the same account across both platforms. By December 2016, Discord had 25 million unique users and was processing over 120 million messages every month.

a. Discord provides free hosting for registered users to set up, configure, and customize their own communication servers, as well as a sleek and intuitive user interface for low-latency voice calls or persistent, Internet Relay Chat (IRC) text chat rooms. Discord aims to provide an all-in-one experience, borrowing and improving upon many of the most popular features of similar services such as Skype and TeamSpeak, as well as adding unique features of its own. Discord can be accessed via web browser or by installing an application for a Windows, iOS, or Android device.

b. In addition to the above features, Discord users can communicate with voice calls, video calls, text messaging, media, and files in private chats or as part of communities called "servers." The information requested Attachment B is maintained by Discord and is the subject of preservation letter number 12588895.

c. New users register for the service with an email address, username, and password; after registering, users have access to all of Discord's features. Users choose an alphanumeric username, which is then combined with a pound symbol (#) as well as a string of 4 or 5 randomized numbers, producing a unique "tag." This tag (example: NW3C_Test#3814) cannot be changed. The tag is

publicly visible on an account's profile and can be used for a variety of networking purposes inside of Discord, such as friend lists, server whitelists, and blocking other users.

d. Users can link other social media, communication, and entertainment services to their Discord account and can automatically integrate features of those applications into their Discord usage. While information found on each of these services is dependent on that user's privacy settings, all Discord profiles are public. Users can connect their Discord account to Steam, Twitch.TV, Reddit, Twitter, and Google+ accounts. Linked accounts can potentially provide investigative leads to law enforcement, as identifying account information can be found on each user's public Discord profile.

15. Based on DISCORD's Privacy Policy, modified March 15, 2024 and available online, I know the following about the collection of preservation of data at Discord:

a. Discord collects information from users when they voluntarily provide information, such as when they register for access to the Discord application and related Internet services (the "Services"). Information Discord collects may include, but is not limited to, username, email address, and any messages, images, transient VOIP data (to enable communication delivery only), or other content users send via the chat feature.

b. When users interact with Discord by using its Services, Discord receives and stores certain information such as an IP address, device ID, and the user's Services activities. Discord may store this information in databases owned and maintained by affiliates, agents or service providers. The Services may use

this information and pool it with other information to track, for example, the total number of visitors to DISCORD's website, the number of messages users have sent, and the domain names of visitors' Internet service providers.

c. Discord may conduct research on its customer demographics, interests, and behavior based on the information collected. This research may be compiled and analyzed on an aggregate basis, and Discord may share this aggregate data with its affiliates, agents, and business partners. Discord may also disclose aggregated user statistics to describe its Services to current and prospective business partners, and to third parties for other lawful purposes.

d. Users may give Discord permission to collect their information in other services. For example, a user may connect a social networking service such as Facebook or Twitter to their Discord account. When a user does this, it allows Discord to obtain information from those accounts (for example, a user's friends or contacts).

e. Discord uses cookies and similar technologies to keep track of users' local computer settings such as notification settings and which account users have logged into the Services. Cookies are pieces of data that sites and services can set on a user's browser or device that can be read on future visits. Discord may expand its use of cookies to save additional data as new features are added to the Services it provides. In addition, Discord uses technologies such as web beacons and single-pixel gifs to record log data such as open rates for emails sent by the system.

f. Discord may use third party website analytic tools such as Google Analytics on its website that use cookies to collect certain information concerning use of its Services. However, users can disable cookies by changing their browser settings.

g. A user may see a Discord Service advertised in other applications or websites. After clicking on one of these advertisements and installing a Discord Service, the user will become a user of the Service. Advertising platforms, which include Twitter and Facebook (and whose software development kits are integrated within Discord's Service), may collect information for optimizing advertising campaigns outside of the Service.

16. In my training and experience, I have learned that providers of e-mail and/or social media services offer a variety of online services to the public. Providers, like Discord, allow subscribers to obtain accounts like the TARGET ACCOUNT. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other e-mail addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

17. Therefore, Discord's computers are likely to contain stored electronic communications and information concerning subscribers and their use of Discord's Services, such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of target account.

18. A subscriber of a service provider, such as Discord, can also store with the service provider files in addition to e-mails or other messages, such as address books, contact or buddy lists, calendar data, pictures or videos (other than ones attached to e-mails), notes, and other files, on servers maintained and/or owned by the service provider. In my training and experience, evidence of who was using an account may be found in such information.

19. In my training and experience, e-mail and social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail and social media providers often have records of the IP address used to register the account and the IP addresses associated with logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the target account.

20. In my training and experience, e-mail and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of e-mails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the target account.

21. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often need to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces of information will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with enough information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and

control of that account. For the purpose of searching for content demonstrating the actual user(s) of the TARGET ACCOUNT, I am requesting a warrant requiring Discord to turn over all information associated with the TARGET ACCOUNT with the date restriction included in Attachment B for review by the search team.

22. Relatedly, the government must be allowed to determine whether other individuals had access to the TARGET ACCOUNT. If the government were constrained to review only a small subsection of an account, that small subsection might give the misleading impression that only a single user had access to the account.

23. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images, emojis and emoticons—images or computer-key configurations used to express a concept or idea, such as a happy face inserted into the content of a message or the use of a colon and parenthesis :) to convey a smile or agreement—to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

24. In my training and experience, providers also keep a record of search queries run by the user of the account, whether searches within the services of the provider for persons, content, or other accounts (such as if a user is trying to find the account of an acquaintance), or

broader Internet searches. In some instances, providers may also keep records of which websites or contents were "clicked on" as a result of these searches. This information is helpful both in the context of the case to show the topics about which the user was trying to obtain more information or conduct research, and is relevant for "user attribution" evidence, analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

25. I know based on my training and experience that providers of e-mail or social media services generally have access to and store the web or Internet browsing history of the user while he or she is logged into an account. That history can include names and specific websites or URLs/URIs (Uniform Resource Locators or Indicators) of the sites that have been visited.

26. I know based on my training and experience that providers of e-mail or social media services will often keep track of what is referred to as user agent string, which contains information about the type of computer, operating system, and web browser used to access the service. User agent string can include: web requests or HTTP requests (hypertext transfer protocol is the protocol by which many web pages are transmitted between servers and clients or users); logs containing information such as the requestor's IP address, identity and user ID, date and timestamp, request URL or URI (website address), HTTP protocol version, referrer, and similar information; login tracker logs; account management logs; and any other e-mail or social media accounts accessed by or analytics related to the target account. These can be used to determine the types of devices used while accessing the target account, as well as data related to the user's activity while accessing the target account.

27. Users of accounts are often required to include an e-mail account as well as a phone number in subscriber records. The e-mail account may be an e-mail account hosted at the

same provider, or an account at a different provider. The e-mail account is referred to by several names, such as a secondary e-mail account, a recovery e-mail account, or an alternative e-mail account or communication channel. That e-mail account is often used when the identity of the user of the primary account (the target account) needs to be verified, for example if a password is forgotten, so that the provider can confirm that the person trying to access the account is the authorized user of the account. Similarly, the telephone number used in subscriber records is often used to send a passcode via text (or "SMS") that must be presented when trying to gain access to an account, either in a similar scenario where a user forgot his or her password, or when users implement what is referred to as "two-factor authentication" (where the password is one factor, and the passcode sent via text message to a mobile device is a second). In either scenario, the user of a primary e-mail account (target account) and a secondary e-mail account or phone number listed in subscriber records are very often the same person, or at least are close and trusted and/or working in concert. That is because access to either the secondary e-mail account or to the phone number listed in subscriber records can allow access to the primary account.

28. Providers also frequently obtain information about the types of devices that are used to access accounts like the TARGET ACCOUNT. Those devices can be laptop or desktop computers, cellular phones, tablet computers, or other devices. Individual computers or devices are identified by a number of different means, some of which are assigned to a particular device by a manufacturer and connected to the "hardware" or the physical device, some are assigned by a cellular telephone carrier to a particular account using cellular data or voice services, and some are actually assigned by the provider to keep track of the devices using its services. Those device identifiers include Android IDs, Advertising IDs, unique application numbers, hardware

models, operating system versions, unique device identifiers, Global Unique Identifiers or "GUIDs," serial numbers, mobile network information, phone numbers, device serial numbers, Media Access Control ("MAC") addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"). Apple, one of the primary suppliers of mobile devices used to access accounts like the TARGET ACCOUNT, had previously used an identifier that was unique to the hardware of its devices, such that details of a device's activity obtained from a particular application or "app" could be used to target advertisements for the user of that device. Apple replaced that hardware-based identifier with the Apple advertiser ID or IDFA that is still unique to a device, but which can be wiped and re-generated by a user if a user chooses to do so. Most users, however, do not know that the IDFA exists, and therefore are unaware that their device's activity can be correlated across different apps or services.

29. These device identifiers can then be used (a) to identify accounts accessed at other providers by that same device, and (b) to determine whether any physical devices found during the investigation were the ones used to access each target account. The requested Warrant therefore asks for the device identifiers, as well as the identity of any other account accessed by a device with the same identifier.

30. Providers of e-mail and social media often maintain, have access to, and store information related to the location of the users of accounts they service. That information may be obtained by the provider in several ways. For example, a user may access the provider's

services by running an application on the user's phone or mobile device, which application has access to the location information residing on the phone or mobile device, such as Global Positioning System (GPS) information. It may also be accessible through "check-in" features that some providers offer that allow users to transmit or display their location to their "friends" or "acquaintances" via the provider.

31. The subscriber will also generally need to use a password that will allow the user to gain access to the account. Many providers do not store the password directly, rather they use an algorithm (often referred to as a "hashing" algorithm) that is performed on the password and generates a new random of string of numbers and characters, which is what the provider may store. When a user enters his or her password, the hashing algorithm is performed on the password before it is presented to the provider, and the provider will verify the hash value for the password (rather than the password itself) to authorize access to the account. As an added security feature, some providers insert additional text before or after the password, which is referred to as "salting" the password. The hashing algorithm is then performed on the combined password and salt, which is the hash value that will be recognized by the provider. Alternatively, or in addition to passwords, users may be required to select or propose a security question, and then provide an answer, which can be used to substitute for a password or to retrieve or reset a user's password.

32. This Application seeks a warrant to search all responsive records and information under the control of the service provider, which is subject to the jurisdiction of this Court, regardless of where the provider has chosen to store such information.

33. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from Discord, under seal, until the investigation is

completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

34. I make that request because I believe it might be impossible for a provider to authenticate information taken from the target account as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a document found by the search team and confirm that it was a business record of the provider taken from the target account.

35. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it—and its contents—may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not access his or her account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

## CHILD PORNOGRAPHY

## COLLECTOR/TRAFFICKER CHARACTERISTICS

36. Based on my experience, training, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain common characteristics are often present in individuals who collect or traffic child pornography.

I have observed and/or learned about the reliability of these commonalities and conclusions involving individuals who collect, produce, and solicit images of child pornography. The following are those traits and characteristics of individuals who traffic child pornography:

a. Many individuals who produce, solicit, and traffic images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect or traffic in child pornography also collect and seek to access other sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect and access child erotica, which may consist of images or text that do not meet the legal definition of child pornography, but which nonetheless fuel their sexual fantasies involving children.

c. Many individuals who collect, produce, solicit, and traffic in child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest in children and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to,

Peer-to-Peer (P2P), email, email groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

37. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect, solicit, produce, or traffic child pornography often do not willfully dispose of their child pornography materials, even after contact with law enforcement officials.

## BACKGROUND OF THE INVESTIGATION AND STATEMENT OF PROBABLE CAUSE

38. March 21, 2024, Calais Police Department referred an incident to me regarding an allegation that Kuhas Polchies was impersonating an individual (V1) and had transmitted, unsolicited, child sexual abuse material (CSAM) that he produced of V1 to another Facebook user.

39. I reviewed screenshots provided by Calais Police Department of a Facebook Messenger chat that appeared to take place on February 20, 2024. The text chat was between an individual (FACEBOOK USER 1), that is alleged to be Polchies, who was using a Facebook account that appeared to belong to V1 (FACEBOOK ACCOUNT 1/FA1). In this chat, FACEBOOK USER 1, using FA1, transmitted what appeared to be sexually explicit photos and videos of V1 via Facebook Messenger as part of an unsolicited sexting chat.

40. V1 stated during an interview that all referenced images and videos transmitted by FACEBOOK USER 1 that depict V1 with blue dyed hair, or include depictions of V1's genitals, were produced by Polchies when V1 was 15 years old.

## LINKING FACEBOOK ACCOUNT 1 (FA1) TO POLCHIES

41. On or about April 29, 2024, I requested preservations and subpoenas be sent to Meta Platforms for subscriber/account information, including name, date of birth, address, phone number, email address, registration date, registration IP address, and any other identifying information, as well as all IP logins, for the period April 29, 2022 to April 29, 2024 for the following Facebook profiles:

- Unique ID ending in 1010 (FA1; the account from which the above photos and videos were transmitted on February 20, 2024).
- Unique ID ending in 5267 (FA2; another account that previously to belonged to V1 is alleged to now be controlled by Polchies and inaccessible to V1.).
- Unique ID ending in 5638 with vanity name "kuhas.polchies" (FA3; a Facebook account that allegedly belongs to the Polchies). The Facebook subpoena return included phone number(s) provided by the account holder. "Verified" indicates the account holder responded to a text sent to the listed phone number to verify control over the phone number. Cellular phone number 207-214-8210 was verified on June, 26, 2020 according to the subpoena return, which is the most recent phone number verified on this account.
- Unique ID ending in 0736 with vanity name "kuhas.polchies.908" (FA4; a second Facebook account that allegedly belongs to the subject).

42. On April 29, 2024, pursuant to Administrative Subpoena 959441, served via email on the same date, Pioneer Broadband provided subscriber information for several IP addresses associated with repeatedly logging into and out of the above referenced Facebook

accounts. An excerpt of Facebook in/out information below illustrates user overlap among the above referenced Facebook accounts:

- 74.221.77.201 on 4/22/2024 at 14:29:16 UTC [gleaned from Facebook account, unique ID ending in 1010 (FA1)]
- 74.221.77.201 on 4/22/2024 at 14:28:38 UTC [gleaned from the "Kuhas Polchies" Facebook account, vanity name kuhas.polchies, unique ID ending in 5638 (FA3)]
- 74.221.75.123 on 3/22/2024 at 10:11:24 UTC [gleaned from Facebook account, unique ID ending in 1010 (FA1)]
- 74.221.75.123 on 3/22/2024 at 10:11:25 UTC [gleaned from the "Kuhas Polchies" Facebook account, vanity name kuhas.polchies, unique ID ending in 5638 (FA3)]
- 74.221.75.123 on 3/22/2024 at 11:05:47 UTC [gleaned from the "Kuhas Polchies" Facebook account, vanity name kuhas.polchies.908, unique ID ending in 0736 (FA4)]
- 74.221.75.123 on 2/20/2024 at 14:55:41 UTC [gleaned from Facebook account, unique ID ending in 1010 (FA1)]
- 64.89.247.167 on 4/5/2024 at 23:32:44 UTC [gleaned from Facebook account, unique ID ending in 1010 (FA1)]
- 64.89.247.167 on 4/5/2024 at 23:58:24 UTC [gleaned from the "Kuhas Polchies" Facebook account, vanity name kuhas.polchies, unique ID ending in 5638 (FA3)]

43. The Pioneer Broadband response showed that all above referenced IP addresses resolved to an account in the name of Kuhas Polchies at a residence in Indian Township, Maine.

## SEARCH WARRANT EXECUTION

44. On May 23, 2024, the Federal Bureau of Investigation (FBI) executed a search warrant at Polchies' residence in Indian Township, Maine, the same address associated with his Pioneer service. While the residential search warrant was underway, Polchies stated, during a voluntary, non-custodial interview with me and FBI Special Agent Jose Rodriguez-Aguilar, that he regularly clicks on links posted on Reddit and Telegram that navigate to websites containing child pornography, among other types of pornography. However, Polchies said he only clicks on these links to look at pornography depicting adults above the age of 18 years old.

45. Polchies said during a non-custodial, voluntary interview with FBI Special Agent Marc Toulouse that he and V1 have known each other since elementary school and started dating when V1 was fifteen years old and Polchies was twenty years old. Polchies said he started taking pictures and videos of V1 when she was 16 years old and Polchies was 21 years old. Polchies said that he sent sexually explicit pictures and videos of both he and V1 as well as just V1 while using V1's old Facebook account that he still had access to at the time of the search warrant. Polchies estimated that he used V1's account to send pictures and videos to five different social media accounts that he found in V1's Facebook contacts. Polchies further said that the pictures and videos consisted of pictures of V1's breasts and buttocks and some videos of her masturbating, but could not remember exactly what he sent. He estimated that he sent a total of one hundred pictures and videos to the five different accounts, and of those pictures and videos, fifteen to twenty were of V1 when they were sixteen years old.

46. Polchies also said that he sent fifty to one hundred pictures and videos of V1 using one of his social media accounts. Of the fifty to one hundred pictures and videos, he estimated that fifteen to twenty were of V1 when they were sixteen years old.

47. Polchies remembered taking naked pictures of V1 in a tiny house and at his father's residence in Waite, Maine.

## IDENTIFICATION OF CHILD SEXUAL ABUSE MATERIAL

48. Based on the above facts and upon review of the images, four photos and two screenshots of videos transmitted by FA1 on about February 20, 2024 appeared to constitute child pornography as defined by 18 U.S.C. § 2256(2)(A)(v) as lascivious exhibition of the anus, genitals, or pubic area of any person. One of these is a nude photo of V1 with blue dyed hair laying on her back with their legs spread apart to show a close-up image of her exposed vagina. This image or an image taken at the same time was later recovered from Polchies' iPhone as described below as Exhibit 1.

49. On May 23, 2024, the day of the search warrant, I conducted a cursory preview of two smart phones that were located under a laundry basket in what appeared to be Polchies' bedroom closet to attempt to identify the sexually explicit images of V1 that were allegedly transmitted by Polchies on Facebook using V1's Facebook account. While previewing Polchies' phone camera rolls, I saw numerous pornographic images of young women, many of which it could not be determined by cursory review to be above the age of 18 years old.

50. While scrolling through the black iPhone camera roll, I located multiple images in the phone camera roll that appeared identical to the referenced images in the Facebook communications, including Exhibit 1.

51. I entered the interview room where Polchies was being interviewed by SA Tolouse. After confirming the phones belonged to Polchies, I showed Polchies three nude images of V1 that appeared identical to those that were sent from V1's Facebook account. Polchies said he took all three pictures with his phone. I then showed Polchies the date time stamp that was readily visible at the top of each of the three referenced images of V1 in the camera roll and asked Polchies, based on the dates, "wouldn't that make [V1] fifteen when you took the pictures?" Polchies agreed that would be true.

52. These and other images of V1 were also identified in a forensic search of the phone described above. Exhibit 1 is an image, with a creation date of December 20, 2017, that appears identical to the image described in Paragraph 45, above. This image was in the user accessible space on the phone. EXIF data from this phone indicates that it was produced using an iPhone 7. I know from experience that all iPhones are manufactured outside the United States.

53. The forensic review of an iPhone seized from Polchies also revealed dozens of images of child pornography associated with the use of the Telegram messaging app. Telegram is a foreign-based, end-to-end encrypted application that uses the internet to share communication, including images and videos. The forensic data associated with these images indicate that they came to Polchies' device at various times, with a large concentration of activity in January 2024.

## DISCORD ACTIVITY

54. Polchies said during an interview on October 28, 2024 that he posted CSAM of V1 on Discord chats. Polchies also verified his Discord username was "bokunobubbles" and said his Discord account was registered to his email address kuhaspolchies@yahoo.com. A forensic review of an iPhone seized from Polchies revealed a Discord account that appeared to be

controlled by POLCHIES with vanity name "bokunobubbles," which contained a chat where POLCHIES was an active participant and users appeared to be sharing pornographic images of people in the local Maine community [Exhibit 2]. Multiple users in a partially extracted Discord chat from Polchies' iPhone appeared to ask for and state the real names of people whose pornographic images were being posted in the chat. Polchies said he associated V1's name with the images and videos he posted of V1 on Discord. A message posted on the chat by user "@biguydan#0" on May 12, 2024 specifically named the first initial and last name of V1 [Exhibit 3]. Messages from the referenced chat from the limited Discord data extraction spanned February 21, 2023 to May 22, 2024. Six pornographic photos from Polchies' iPhone and identified as depicting V1 have file names and locations indicating the photos were stored in and extracted from Discord files [Exhibits 4 through 9]. V1 was identified to be under the age of 18 years old in three of five images, and the age of V1 in the remaining two images is unknown at this time. The "created dates" of these photos were between September 16, 2023 and September 18, 2023, which coincides with the timeframe where Polchies appears to have been active on the referenced Discord chat based on the phone extraction data. On November 25, 2024, pursuant to Administrative Subpoena 1009588, served via the Kodex Portal on November 22, 2024, Discord provided subscriber information and IP logins for the Discord account associated with email address kuhaspolcies@yahoo.com for the time period January 1, 2023 to June 1, 2024:

a. User ID: 459434556081176576

b. Username: bokunobubbles#0

c. Email: kuhaspolchies@yahoo.com

## CONCLUSION

55. Based on the above, I have probable cause to believe Polchies knowingly possessed child pornography as defined in Title 18, United States Code, Section 2256(8)(A), that had been shipped and transported in interstate and foreign commerce by any means, including by computer, and were produced using materials that had moved in interstate and foreign commerce, and that he distributed images of CSAM on Discord. Evidence of the crime is likely to be found in data associated with Polchies' Discord account. Accordingly, I respectfully request the Court to issue the Warrant.

56. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this Warrant. The government will execute this warrant by serving it on Discord. Because the warrant will be served on Discord, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

57. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Craig S. Mehrmann
Special Agent
Federal Bureau of Investigation

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedure

Date: Dec 03 2024

City and state: Bangor, ME

Judge's signature

John C Nivison U.S. Magistrate Judge
Printed name and title